(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 51 012 A 1**

(51) Int. Cl.[7]: **G 06 F 11/30**
G 06 F 1/24

(21) Aktenzeichen: 101 51 012.8
(22) Anmeldetag: 16. 10. 2001
(43) Offenlegungstag: 17. 4. 2003

(71) Anmelder:
Volkswagen AG, 38440 Wolfsburg, DE

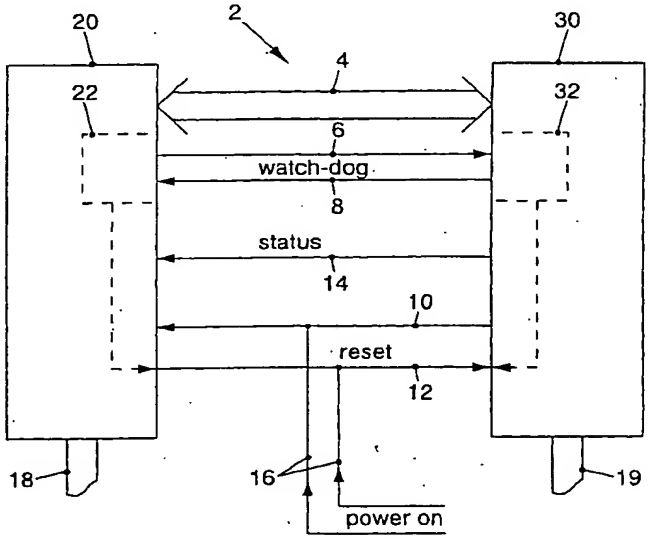
(72) Erfinder:
Altenkirch, Manfred, 38553 Wasbüttel, DE; Klinkig, Andreas, 38162 Cremlingen, DE; Löhner, Andreas, 38154 Königslutter, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:
DE 40 04 709 C2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Rechnersystem

(57) Es wird ein Verfahren zum Überwachen eines Rechnersystems mit wenigstens einer ersten und einer zweiten Recheneinheit, die sich gegenseitig überwachen, vorgeschlagen, bei dem zwischen der ersten und der zweiten Recheneinheit (20, 30) über erste Signalleitungen (6, 8) Daten und/oder Steuersignale übertragen werden; jede Recheneinheit (20, 30) die von der anderen Recheneinheit (30, 20) übertragenen Daten und/oder Steuersignale zum Erkennen eines fehlerhaften Zustandes der anderen Recheneinheit (30, 20) überprüft; bei Erkennen eines fehlerhaften Zustandes einer der Recheneinheiten (20, 30) durch die andere Recheneinheit (30, 20) von der anderen Recheneinheit über zweite Signalleitungen (12, 10) einen Rücksetzimpuls (Reset) zum Neustarten der einen Recheneinheit (20, 30) übertragen wird und das Rechnersystem (2) bei Inbetriebnahme durch Zuführen eines Rücksetzimpulses (Power-On-Reset) zu den Recheneinheiten (20, 30) initialisiert wird. Zur Erhöhung der Funktionssicherheit des Rechnersystems (2) wird während des Initialisierungsvorgangs bei Inbetriebnahme des Rechnersystems (2) die Funktion des gegenseitigen Neustartens der Recheneinheiten (20, 30) durch Übertragen von Rücksetzimpulsen über die zweiten Signalleitungen (10, 12) auf Fehler überprüft.



DE 101 51 012 A 1

DE 101 51 012 A 1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Überwachen eines Rechnersystems mit wenigstens zwei Recheneinheiten, die sich gegenseitig überwachen, gemäß dem Oberbegriff von Patentanspruch 1 sowie ein Rechnersystem mit wenigstens zwei Recheneinheiten, die sich gegenseitig überwachen, gemäß dem Oberbegriff von Patentanspruch 9.

[0002] Derartige eigensichere Rechnersysteme weisen im allgemeinen wenigstens zwei Recheneinheiten bzw. Prozessoren auf, die sich im Normalbetrieb gegenseitig überwachen. Erkennt eine Recheneinheit bei der anderen Recheneinheit eine Fehlfunktion, so muss das Rechnersystem in einen sicheren Zustand versetzt werden. Dies geschieht üblicherweise dadurch, dass beide Recheneinheiten, zumindest aber die als fehlerhaft erkannte Recheneinheit, durch einen Hardware-Reset zurückgesetzt werden, so dass sie wieder in einem definierten Zustand beginnen können. Solche Rechnersysteme werden beispielsweise in sicherheitsrelevanten Bereichen in Kraftfahrzeugen eingesetzt, wie beispielsweise Airbag- oder Gurtstraffersystemen, der elektronischen Steuerung der Brennkraftmaschine, elektronischen Bremsanlagen und dergleichen.

[0003] Ein Rechnersystem und ein Verfahren zum Überwachen des Rechnersystems der eingangs genannten Art sind beispielsweise aus der DE 37 26 489 A1 bekannt. Dort ist ein Rechnersystem zur Steuerung eines Betriebsparameters einer Brennkraftmaschine eines Kraftfahrzeuges bestehend aus zwei Prozessoren, die über ein Signalleitungssystem zum Austausch von Daten und Steuer- bzw. Kontrollsignalen verbunden sind, vorgeschlagen. Zur gegenseitigen Überwachung der beiden Prozessoren ist jeder Prozessor mit einem sogenannten Watch-Dog ausgestattet, der an den jeweils anderen Rechner Kontrollsignale abgibt, anhand derer der jeweils andere Rechner die Funktionsfähigkeit des das Kontrollsignal aussendenden Rechners überprüfen kann. Ein zweiter Überwachungspfad wird bei einem derartigen Zwei-Rechner-System durch die Übertragung von Daten zwischen den beiden Prozessoren aufgebaut. Die Datenübertragung erfolgt zyklisch in einem festen Zeitraster, so dass bei Ausbleiben einer Datenübertragung bzw. -anforderung eines der beiden Rechner der jeweils andere auf einen Funktionsfehler schließen und den fehlerhaften Rechner über einen Reset-Impuls neu starten (Warmstart) kann. Bei Inbetriebnahme des Rechnersystems wird ein beiden Rechnern gemeinsamer Initialisierungsimpuls (Power On) erzeugt, der beide Rechner gleichzeitig zur Initialisierung zurücksetzt (Kaltstart).

[0004] Eine Weiterentwicklung dieses Rechnersystems ist in der DE 40 04 709 A1 derselben Anmelderin offenbart. Um zu verhindern, dass das aus der DE 37 26 489 A1 bekannte Rechnersystem nicht ordnungsgemäß in Betrieb genommen werden kann, wenn der gemeinsame Initialisierungsimpuls bzw. die diesen Initialisierungsimpuls erzeugende Schaltungsanordnung fehlerbehaftet ist, ist bei dem dort beschriebenen Rechnersystem eine von der den Initialisierungsimpuls erzeugenden Schaltungsanordnung unabhängige Einheit vorgesehen, die auch bei Ausfall der Schaltungsanordnung einen Rücksetzimpuls an die beiden Recheneinheiten abgeben kann.

[0005] Des weiteren ist aus der DE 198 45 220 A1 ein Rechnersystem bekannt, das einen Rechner aufweist, der über Reset-Signalleitungen und Watch-Dog-Signalleitungen mit mehreren Peripheriegeräten verbunden ist. Der Rechner sendet an die Peripheriegeräte sogenannte Watch-Dog-Signale aus, bei deren Ausbleiben die Peripheriegeräte über die Reset-Signalleitungen an den Rechner einen Rücksetzimpuls (Reset) ausgeben. Um zu vermeiden, dass das Rechnersystem aufgrund zeitversetzt erzeugter Rücksetzimpulse in der Hochlaufphase des Systems hängen bleibt, werden die Watch-Dog-Vorrichtungen der Peripheriegeräte und des Rechners unmittelbar nach dem Hochlaufen des Systems synchronisiert.

[0006] Ausgehend von dem vorgenannten Stand der Technik liegt der vorliegenden Erfindung die Aufgabe zugrunde, ein eigensicheres Rechnersystem und ein Verfahren zum Überwachen eines eigensicheren Rechnersystems bereitzustellen, die eine größere Funktionssicherheit des Rechnersystems gewährleisten.

[0007] Diese Aufgabe wird durch ein Verfahren zum Überwachen eines eigensicheren Rechnersystems mit den Merkmalen von Patentanspruch 1 bzw. durch ein eigensicheres Rechnersystem mit den Merkmalen von Patentanspruch 9 gelöst. Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung sind in den Unteransprüchen 2–8 bzw. 10–16 definiert.

[0008] Bei dem eigensicheren Rechnersystem gemäß der vorliegenden Erfindung werden über erste Signalleitungen zwischen der ersten und der zweiten Recheneinheit Daten und/oder Steuersignale übertragen; jede Recheneinh überprüft mittels einer entsprechenden Vorrichtung die von der anderen Recheneinheit übertragenen Daten und/oder Steuersignale zum Erkennen eines fehlerhaften Zustandes der anderen Recheneinheit; bei Erkennen eines fehlerhaften Zustandes einer der Recheneinheiten durch die andere Recheneinheit wird von der anderen Recheneinheit über zweite Signalleitungen einen Rücksetzimpuls (Reset) zum Neustarten der einen Recheneinheit übertragen; und das Rechnersystem wird bei Inbetriebnahme durch Zuführen eines Rücksetzimpulses (Power-On-Reset) über eine entsprechende Signalleitung zu den Recheneinheiten initialisiert, wobei während des Initialisierungsvorgangs bei Inbetriebnahme des Rechnersystems die Funktion des gegenseitigen Neustartens der Recheneinheiten durch Übertragen von Rücksetzimpulsen über die zweiten Signalleitungen auf Fehler überprüft wird. Dadurch, dass bei jeder Inbetriebnahme des Rechnersystems die Funktion des gegenseitigen Neustartens der Recheneinheiten überprüft wird, wird die Betriebssicherheit des Rechnersystems deutlich erhöht. Ein Rechnersystem, bei dem diese für die Sicherheit unbedingt erforderliche Funktion des gegenseitigen Neustartens der Recheneinheiten als fehlerbehaftet erkannt wird, kann nicht in Betrieb genommen werden.

[0009] Diese Funktionsprüfung kann dadurch erfolgen, dass während des Initialisierungsvorgangs bei Inbetriebnahme des Rechnersystems die Recheneinheiten nacheinander durch einen Rücksetzimpuls von der jeweils anderen Recheneinheit neu gestartet werden und der Initialisierungsvorgang nur abgeschlossen wird, wenn die Funktion des gegenseitigen Neustartens der Recheneinheiten als fehlerfrei festgestellt worden ist.

[0010] Zur Durchführung der Funktionsprüfung ist es vorteilhaft, der ersten Recheneinheit von der zweiten Recheneinheit über die erste Signalleitung oder eine zusätzliche Signalleitung ein Steuersignal zuzuführen, welches einen Betriebszustand der zweiten Recheneinheit angibt.

[0011] Je nach Betriebszustand der zweiten Recheneinheit kann dieses Steuersignal zu Beginn der Inbetriebnahme des Rechnersystems sowie nach einem erfolgreich abgeschlossenen Initialisierungsvorgang bei Inbetriebnahme des Rechnersystems einen Betriebszustand "vor der Initialisierung" (Init), nach einer als fehlerfrei festgestellten Funktion des gegenseitigen Neustartens der Recheneinheiten während des Initialisierungsvorgangs bei Inbetriebnahme des Rechnersystems einen Betriebszustand "Funktion des gegenseitigen Neustartens als fehlerfrei festgestellt" (Reset ACK) und

bei Erkennen einer fehlerhaften ersten Recheneinheit einen Betriebszustand "Fehler in Recheneinheit erkannt" (Failure detected) angeben. Mit anderen Worten kann der ersten Recheneinheit über die zusätzliche Signalleitung signalisiert werden, ob der Neustart durch einen Power-On-Reset bei Inbetriebnahme des Rechnersystems, die Prüfung der Funktion des gegenseitigen Neustartens der Recheneinheiten oder durch einen festgestellten Fehler ausgelöst wurde.

[0012] Zur weiteren Erhöhung der Sicherheit kann auch noch eine weitere zusätzliche Signalleitung vorgesehen sein, über die der zweiten Recheneinheit von der ersten Recheneinheit in analoger Weise ein Steuersignal zuführbar ist, welches einen Betriebszustand der ersten Recheneinheit angibt. Alternativ kann dieses Steuersignal der zweiten Recheneinheit von der ersten Recheneinheit auch über die erste Signalleitung zugeführt werden.

[0013] Ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung wird nachfolgend anhand der Zeichnungen näher erläutert. Darin zeigen:

[0014] **Fig.** 1 ein stark vereinfachtes Blockschaltbild eines Rechnersystems gemäß einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung; und

[0015] **Fig.** 2 eine schematische Darstellung zur Erläuterung der erfindungsgemäßen Funktionsprüfung bei dem in **Fig.** 1 dargestellten Rechnersystem.

[0016] In **Fig.** 1 ist zunächst ein Blockschaltbild eines Rechnersystems gemäß einem bevorzugten Ausführungsbeispiel der Erfindung in stark vereinfachter Form dargestellt. Die erfindungsgemäße Funktionsweise der Überprüfung der Reset-Pfade des Rechnersystems wird anschließend anhand von **Fig.** 2 näher erläutert.

[0017] Das in **Fig.** 1 dargestellte Rechnersystem **2** weist zwei Recheneinheiten bzw. Prozessoren **20, 30** auf, die sich gegenseitig überwachen. Die erste Recheneinheit **20** wird auch als Hauptrechner oder Main-Prozessor bezeichnet, während die zweite Recheneinheit **30** auch als Zweitrechner oder Safety-Prozessor bezeichnet wird. Es sei an dieser Stelle darauf hingewiesen, dass die vorliegende Erfindung grundsätzlich nicht auf ein Rechnersystem mit zwei Recheneinheiten beschränkt ist, es können vielmehr auch drei oder mehr Recheneinheiten in dem Rechnersystem vorhanden sein, die sich gegenseitig überwachen.

[0018] Beide Recheneinheiten **20, 30** sind mit einem Daten- und Kontrollbus **4** und jeweils einem I/O-Bus **18** bzw. **19** verbunden. Die Recheneinheiten **20, 30** können vorzugsweise unabhängig voneinander arbeiten und mit unterschiedlichen Taktfrequenzen betrieben werden.

[0019] Die Recheneinheiten **20** und **30** sind über erste Signalleitungen **6** und **8** miteinander verbunden, über die Daten und/oder Steuersignale von der einen zu der anderen Recheneinheit übertragen werden können. In jeder Recheneinheit **20, 30** ist eine Vorrichtung **22** bzw. **32** zum Erkennen eines fehlerhaften Zustandes der jeweils anderen Recheneinheit **30, 20** anhand der über die ersten Signalleitungen **6, 8** übertragenen Daten und/oder Steuersignale vorgesehen. Die ersten Signalleitungen **6, 8** werden häufig als Watch-Dog-Signalleitungen zur Übertragung von Watch-Dog-Signalen bezeichnet, welche in den sogenannten Watch-Dogs **22, 32** ausgewertet werden. Derartige Watch-Dog-Konstruktionen sind bereits aus dem Stand der Technik bekannt und werden deshalb an dieser Stelle nicht näher erläutert. Die vorliegende Erfindung ist außerdem nicht auf diese eine spezielle Art des Erkennens eines fehlerhaften Zustandes in einer der Recheneinheiten beschränkt.

[0020] Erkennt einer der Watch-Dogs **22, 32** einen fehlerhaften Zustand der anderen Recheneinheit **20, 30**, so gibt er ein entsprechendes Steuersignal an einen Ausgangsanschluss der Recheneinheit **30, 20** ab, der über eine zweite Signalleitung **12** bzw. **10** mit der anderen Recheneinheit **30, 20** verbunden ist. Über diese zweiten Signalleitungen **10, 12** wird der jeweils als fehlerhaft erkannten Recheneinheit **20, 30** ein Rücksetzimpuls (Reset) zum Neustarten dieser Recheneinheit **20, 30** übertragen.

[0021] Diese zweiten Reset-Signalleitungen **10, 12** sind außerdem mit einer weiteren Signalleitung **16** gekoppelt, über die den beiden Recheneinheiten **20, 30** einen gemeinsamen Rücksetzimpuls (Power-On-Reset) zum Initialisieren der Recheneinheiten **20, 30** bei einer Inbetriebnahme des Rechnersystems **2** zugeführt wird.

[0022] Außerdem ist zwischen den beiden Recheneinheiten **20, 30** des Rechnersystems **2** eine zusätzliche Signalleitung **14** vorgesehen. Über diese zusätzliche Signalleitung **14** kann die zweite Recheneinheit **30** der ersten Recheneinheit **20** ihren Betriebszustand (Status) angeben. Insbesondere wird der ersten Recheneinheit **20** durch diese Status-Signalleitung **14** angezeigt, ob ein Neustart (Reset) der ersten Recheneinheit **20** durch eine Inbetriebnahme des Rechnersystems **2** (Power-On-Reset), durch eine Überprüfung der Reset-Pfade während der Initialisierung des Rechnersystems **2** oder durch einen in der ersten Recheneinheit **20** festgestellten Fehler ausgelöst werden soll. Je nach angezeigtem Betriebszustand reagiert die erste Recheneinheit **20** unterschiedlich auf den ihr zugeführten Rücksetzimpuls, wie dies später anhand von **Fig.** 2 näher beschrieben wird.

[0023] Mit Hilfe dieser Status-Signalleitung **14** können die Reset-Pfade des Rechnersystems **2**, d. h. insbesondere die zweiten Reset-Signalleitungen **10, 12** mit den entsprechenden Ein- und Ausgängen an den Recheneinheiten **20, 30**, auf einfache Weise und ohne wesentliche Zeitverzögerung während der Initialisierung der Recheneinheiten **20, 30** bei Inbetriebnahme des Rechnersystems **2** auf ihre Funktion überprüft werden. Nur wenn eine fehlerfreie Funktion der Reset-Pfade des Rechnersystems **2** festgestellt worden ist, wird die Initialisierung abgeschlossen und das Rechnersystem **2** kann zu arbeiten beginnen.

[0024] Zusätzlich kann auch die erste Recheneinheit **20** der zweiten Recheneinheit **30** ihren Betriebszustand in analoger Weise über eine entsprechende zweite Status-Signalleitung (nicht dargestellt) anzeigen. Hierdurch kann die Funktionssicherheit des Rechnersystems **2** wahlweise weiter erhöht werden. Anstelle von einer oder zwei zusätzlichen Signalleitungen können zur Übertragung der Status-Steuersignal zwischen den beiden Recheneinheiten **20, 30** auch die bereits vorhandenen ersten Signalleitungen **6** und **8** verwendet werden.

[0025] Der Ablauf eines erfindungsgemäßen Initialisierungsvorgangs bei dem in **Fig.** 1 dargestellten Rechnersystem **2** wird nun anhand von **Fig.** 2 erläutert.

[0026] Zunächst wird zur Inbetriebnahme des Rechnersystems den Recheneinheiten **20, 30** des Rechnersystems **2** über die Signalleitung **16** ein Rücksetzimpuls (Power-On-Reset) zugeführt (Schritt M1/S1), so dass die beiden Recheneinheiten **20, 30** beginnen hochzufahren. Die Status-Signalleitung **14** hat zu diesem Zeitpunkt einen Signalpegel, der dem Betriebszustand "vor der Initialisierung" (Init) angibt. Die erste Recheneinheit **20** überprüft den Signalpegel der Status-Signalleitung **14** und, da diese einen Betriebszustand "Init" anzeigt, sendet der zweiten Recheneinheit **30** über die entsprechende Reset-Signalleitung **12** einen Rücksetzimpuls (Schritt M2), um anschließend abzuwarten (Schritt M3).

[0027] Aufgrund des über die Reset-Signalleitung **12** empfangenen Rücksetzimpulses (Reset) startet die zweite Recheneinheit **30** erneut (Schritt S2) und beginnt mit der ersten Phase der Initialisierung (Schritt S3).

[0028] Nach einer gewissen Zeitdauer setzt die zweite Re-

cheneinheit **30** den Signalpegel der Status-Signalleitung **14** auf einen Wert Reset ACK" und sendet der ersten Recheneinheit **20** über die entsprechende Reset-Signalleitung **10** einen Rücksetzimpuls (Schritt S4). Aufgrund des über die Reset-Signalleitung **10** empfangenen Rücksetzimpulses (Reset) startet die erste Recheneinheit **20** erneut (Schritt M4). Anhand des der ersten Recheneinheit **20** über die Status-Signalleitung **14** angezeigten Betriebszustandes "Reset ACK" erkennt die erste Recheneinheit **20** außerdem, dass der ihr zugeführte Rücksetzimpuls nach erfolgreicher Prüfung beider Reset-Pfade und nicht beispielsweise bei der Inbetriebnahme des Rechnersystems **2** ausgelöst worden ist. Deshalb löst die erste Recheneinheit **20** nicht, wie in Schritt M2 einen Neustart der zweiten Recheneinheit **30** aus.

[0029] Stattdessen beginnen die beiden Recheneinheiten **20** und **30**, nachdem sie die Zustände der Verfahrensschritte M4 bzw. S4 erreicht haben, nun parallel mit der vollständigen Initialisierung (Schritte M5 bzw. S5), in der u. a. auch ROMs und RAMs überprüft werden können. Im Anschluss daran, d. h. erst nach Überprüfung der Reset-Pfade und vollständiger Initialisierung des Rechnersystems **2** beginnt die normale Programmverarbeitung einschließlich der gegenseitigen Überwachung der beiden Recheneinheiten **20, 30** (Schritte M6 bzw. S6). Der Signalpegel der Status-Signalleitung **14** wird in dieser Phase wieder auf den ursprünglichen Wert "Init" zurückgesetzt, so dass ein durch Unterspannung ausgelöster Neustart des Rechnersystems **2** wieder zu den Betriebszuständen der Schritte M1 und S1 führt.

[0030] Entdeckt die zweite Recheneinheit **30** während der normalen Programmverarbeitung mit gegenseitiger Überwachung mittels der Watch-Dogs **22, 32** einen fehlerhaften Zustand der ersten Recheneinheit **20**, so setzt die zweite Recheneinheit **30** den Signalpegel der Status-Signalleitung **14** auf "Failure detected" und sendet über die Reset-Signalleitung **10** einen Rücksetzimpuls zu der ersten Recheneinheit **20** (Schritt S7). Die erste Recheneinheit **20** wird dadurch neu gestartet (Schritt M7), erkennt aber den Betriebszustand "Failure detected", so dass die erste Recheneinheit **20** die Fehlersituation bemerken und bewerten (Schritt M8) und möglicherweise auch einen Neustart der zweiten Recheneinheit **30** auslösen kann (Schritt M2).

[0031] Wie oben erwähnt, beginnt die normale Programmverarbeitung einschließlich der gegenseitigen Überwachung der beiden Recheneinheiten **20, 30** erst nach Überprüfung der Reset-Pfade und vollständiger Initialisierung des Rechnersystems **2**. Empfängt die erste Recheneinheit **20** während des Initialisierungsvorgangs nicht nach einer vorgegebenen Zeitdauer einen Rücksetzimpuls von der zweiten Recheneinheit (Schritt S4), so erkennt die erste Recheneinheit **20**, dass ein Funktionsfehler in den Reset-Pfaden des Rechnersystems **2** vorliegt. Die erste Recheneinheit **20** kann in diesem Fall das Rechnersystem **2** in einen sicheren Zustand überführen.

[0032] Auf diese Weise wird gewährleistet, dass das Rechnersystem **2** nur in seinen normalen Betriebszustand übergeht, wenn seine Reset-Pfade als fehlerfrei erkannt worden sind. Durch das Rechnersystem gemäß der vorliegenden Erfindung kann es somit nicht vorkommen, dass im Normalbetrieb des Rechnersystems eine der Rechnereinheiten einen Fehler bei der anderen Recheneinheit erkennt, aber aufgrund einer Fehlfunktion in den Reset-Pfaden des Rechnersystems keinen Neustart der fehlerhaften Recheneinheit auslösen kann. Hierdurch wird die Sicherheit des gesamten Rechnersystems deutlich erhöht.

[0033] Ein weiterer Vorteil der Erfindung liegt darin, dass die Reset-Pfade des Rechnersystems ohne großen Aufwand direkt auf ihre Funktionssicherheit geprüft werden können. Die Überprüfung gemäß dem erfindungsgemäßen Verfahren verlängert die Initialisierung des Rechnersystems bei dessen Inbetriebnahme nur unwesentlich.

BEZUGSZEICHENLISTE

2 Rechnersystem
4 Daten- und Kontrollbus
6, 8 erste Signalleitungen (Watch-Dog)
10, 12 zweite Signalleitungen (Reset)
14 zusätzliche Signalleitung (Status)
16 (Power-On-Reset)-Signalleitung
18 I/O-Bus
19 I/O-Bus
20 erste Recheneinheit
22 Fehlererkennungsvorrichtung
30 zweite Recheneinheit
32 Fehlererkennungsvorrichtung

Patentansprüche

1. Verfahren zum Überwachen eines Rechnersystems mit wenigstens einer ersten und einer zweiten Rechc einheit, die sich gegenseitig überwachen, wobei
zwischen der ersten und der zweiten Recheneinheit (**20, 30**) über erste Signalleitungen (**6, 8**) Daten und/oder Steuersignale übertragen werden;
jede Recheneinheit (**20, 30**) die von der anderen Recheneinheit (**30, 20**) übertragenen Daten und/oder Steuersignale zum Erkennen eines fehlerhaften Zustandes der anderen Recheneinheit (**30, 20**) überprüft;
bei Erkennen eines fehlerhaften Zustandes einer der Recheneinheiten (**20, 30**) durch die andere Recheneinheit (**30, 20**) von der anderen Recheneinheit über zweite Signalleitungen (**12, 10**) ein Rücksetzimpuls (Reset) zum Neustarten der einen Recheneinheit (**20, 30**) übertragen wird; und
das Rechnersystem (**2**) bei Inbetriebnahme durch Zuführen eines Rücksetzimpulses (Power-On-Reset) zu den Recheneinheiten (**20, 30**) initialisiert wird,
dadurch gekennzeichnet,
dass während des Initialisierungsvorgangs bei Inbetriebnahme des Rechnersystems (**2**) die Funktion des gegenseitigen Neustartens der Recheneinheiten (**20, 30**) durch Übertragen von Rücksetzimpulsen über die zweiten Signalleitungen (**10, 12**) auf Fehler überprüft wird.

2. Verfahren zum Überwachen eines Rechnersystems nach Anspruch 1, dadurch gekennzeichnet, dass der Initialisierungsvorgang bei Inbetriebnahme des Rechnersystems (**2**) nur abgeschlossen wird, wenn die Funktion des gegenseitigen Neustartens der Recheneinheiten (**20, 30**) als fehlerfrei festgestellt worden ist.

3. Verfahren zum Überwachen eines Rechnersystems nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass während des Initialisierungsvorgangs bei Inbetriebnahme des Rechnersystems (**2**) die Recheneinheiten (**20, 30**) nacheinander durch einen Rücksetzimpuls von der jeweils anderen Recheneinheit neu gestartet werden.

4. Verfahren zum Überwachen eines Rechnersystems nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass zumindest die zweite Recheneinheit (**30**) der ersten Recheneinheit (**20**) über die erste Signalleitung (**8**) oder eine zusätzliche Signalleitung (**14**) ihren Betriebszustand angibt.

5. Verfahren zum Überwachen eines Rechnersystems nach Anspruch 4, dadurch gekennzeichnet, dass die zweite Recheneinheit (**30**) der ersten Recheneinheit

(20) zu Beginn der Inbetriebnahme des Rechnersystems einen Betriebszustand "vor der Initialisierung" (Init) angibt.

6. Verfahren zum Überwachen eines Rechnersystems nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass die zweite Recheneinheit (30) der ersten Recheneinheit (20) nach einer als fehlerfrei festgestellten Funktion des gegenseitigen Neustartens der Recheneinheiten (20, 30) während des Initialisierungsvorgangs bei Inbetriebnahme des Rechnersystems (2) einen Betriebszustand "Funktion des gegenseitigen Neustartens als fehlerfrei festgestellt" (Reset ACK) angibt.

7. Verfahren zum Überwachen eines Rechnersystems nach einem der Ansprüche 4 bis 6, dadurch gekennzeichnet, dass die zweite Recheneinheit (30) der ersten Recheneinheit (20) nach einem erfolgreich abgeschlossenen Initialisierungsvorgang bei Inbetriebnahme des Rechnersystems (2) einen Betriebszustand "vor der Initialisierung" (Init) angibt.

8. Verfahren zum Überwachen eines Rechnersystems nach einem der Ansprüche 4 bis dadurch gekennzeichnet, dass die zweite Recheneinheit (30) der ersten Recheneinheit (20) bei Erkennen einer fehlerhaften ersten Recheneinheit (20) einen Betriebszustand "Fehler in Recheneinheit erkannt" (Failure detected) angibt.

9. Rechnersystem mit wenigstens einer ersten und einer zweiten Recheneinheit, die sich gegenseitig überwachen, wobei

erste Signalleitungen (6, 8) zur Übertragung von Daten und/oder Steuersignalen zwischen der ersten und der zweiten Recheneinheit (20, 30) vorgesehen sind;

jede Recheneinheit (20, 30) eine Vorrichtung (22, 32) zum Erkennen eines fehlerhaften Zustandes der anderen Recheneinheit (30, 20) anhand der übertragenen Daten und/oder Steuersignale aufweist;

zweite Signalleitungen (10, 12) zur Übertragung von Rücksetzimpulsen (Reset) zwischen der ersten und der zweiten Recheneinheit (20, 30) vorgesehen sind, wobei bei Erkennen eines fehlerhaften Zustandes einer der Recheneinheiten (20, 30) durch die Vorrichtung (32, 22) der anderen Recheneinheit (30, 20) von der anderen Recheneinheit ein Rücksetzimpuls zum Neustarten der einen Recheneinheit (20, 30) übertragen wird; und

eine Signalleitung (16) vorgesehen ist, über die der ersten und der zweiten Recheneinheit (20, 30) ein Rücksetzimpuls (Power-On-Reset) zuführbar ist, um das Rechnersystem (2) bei Inbetriebnahme zu initialisieren, gekennzeichnet durch

eine Einrichtung zum Überprüfen der Funktion des gegenseitigen Neustartens der Recheneinheiten (20, 30) durch Übertragen von Rücksetzimpulsen über die zweiten Signalleitungen (10, 12) während des Initialisierungsvorgangs bei Inbetriebnahme des Rechnersystems (2) auf Fehler.

10. Rechnersystem nach Anspruch 9, dadurch gekennzeichnet, dass der Initialisierungsvorgang bei Inbetriebnahme des Rechnersystems (2) nur abgeschlossen wird, wenn die Funktion des gegenseitigen Neustartens der Recheneinheiten (20, 30) als fehlerfrei festgestellt worden ist.

11. Rechnersystem nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass das Rechnersystem eine zusätzliche Signalleitung (14) aufweist, über die der ersten Recheneinheit (20) von der zweiten Recheneinheit (30) ein Steuersignal zuführbar ist, welches einen Betriebszustand der zweiten Recheneinheit (30) angibt.

12. Rechnersystem nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass der ersten Recheneinheit (20) von der zweiten Recheneinheit (30) über die erste Signalleitung (8) ein Steuersignal zuführbar ist, welches einen Betriebszustand der zweiten Recheneinheit (30) angibt.

13. Rechnersystem nach Anspruch 11 oder 12, dadurch gekennzeichnet, dass über die erste Signalleitung (8) oder die zusätzliche Signalleitung (14) der ersten Recheneinheit (30) von der zweiten Recheneinheit (30) zu Beginn der Inbetriebnahme des Rechnersystems (2) einen Betriebszustand "vor der Initialisierung" (Init) und nach einer als fehlerfrei festgestellten Funktion des gegenseitigen Neustartens der Recheneinheiten (20, 30) während des Initialisierungsvorgangs bei Inbetriebnahme des Rechnersystems (2) einen Betriebszustand "Funktion des gegenseitigen Neustartens als fehlerfrei festgestellt" (Reset ACK) zuführbar ist.

14. Rechnersystem nach einem der Ansprüche 11 bis 13, dadurch gekennzeichnet, dass über die erste Signalleitung (8) oder die zusätzliche Signalleitung (14) der ersten Recheneinheit (30) von der zweiten Recheneinheit (30) bei Erkennen einer fehlerhaften ersten Recheneinheit (20) einen Betriebszustand "Fehler in Recheneinheit erkannt" (Failure detected) zuführbar ist.

15. Rechnersystem nach einem der Ansprüche 9 bis 14, dadurch gekennzeichnet, dass das Rechnersystem eine weitere zusätzliche Signalleitung aufweist, über die der zweiten Recheneinheit (30) von der ersten Recheneinheit (20) ein Steuersignal zuführbar ist, welches einen Betriebszustand der ersten Recheneinheit (20) angibt.

16. Rechnersystem nach einem der Ansprüche 9 bis 14, dadurch gekennzeichnet, dass der zweiten Recheneinheit (30) von der ersten Recheneinheit (20) über die erste Signalleitung (6) ein Steuersignal zuführbar ist, welches einen Betriebszustand der ersten Recheneinheit (20) angibt.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 101 51 012 A1
Int. Cl.[7]: G 06 F 11/30
Offenlegungstag: 17. April 2003

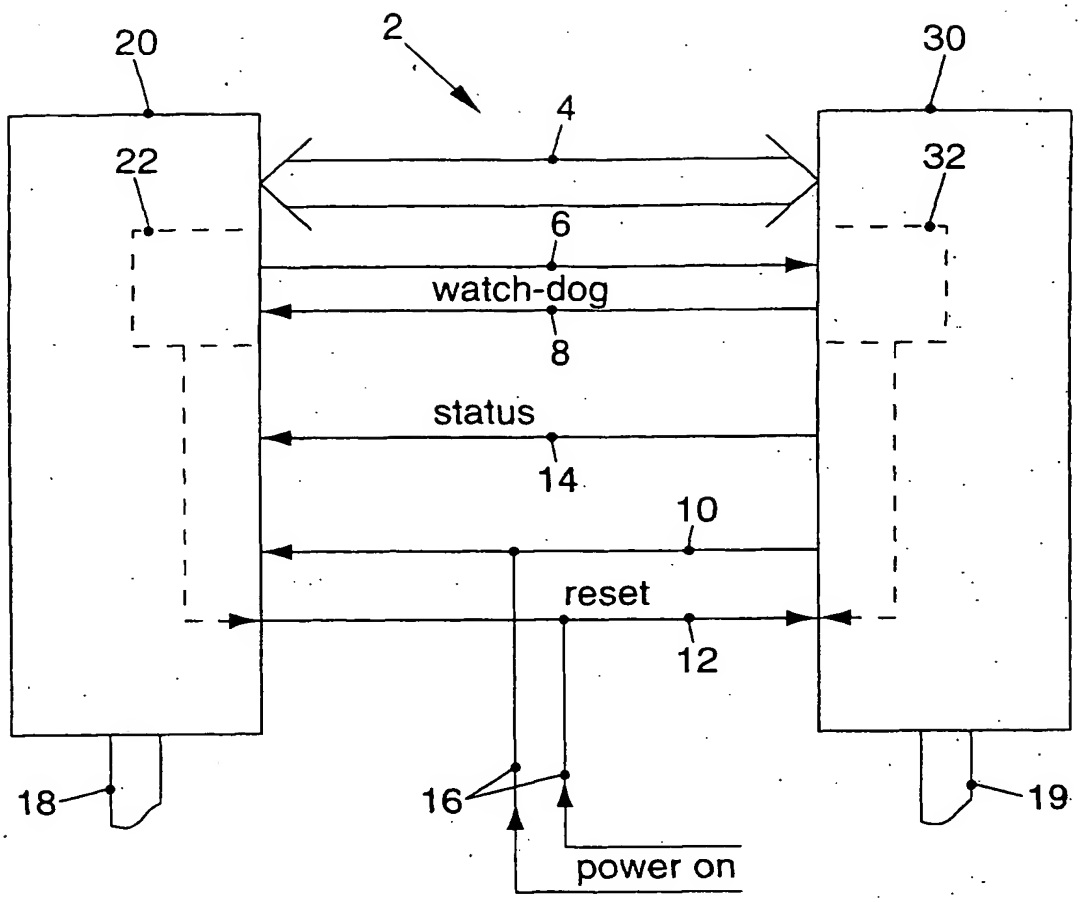


FIG. 1

Nummer: DE 101 51 012 A1
Int. Cl.: G 06 F 11/30
Offenlegungstag: 17. April 2003

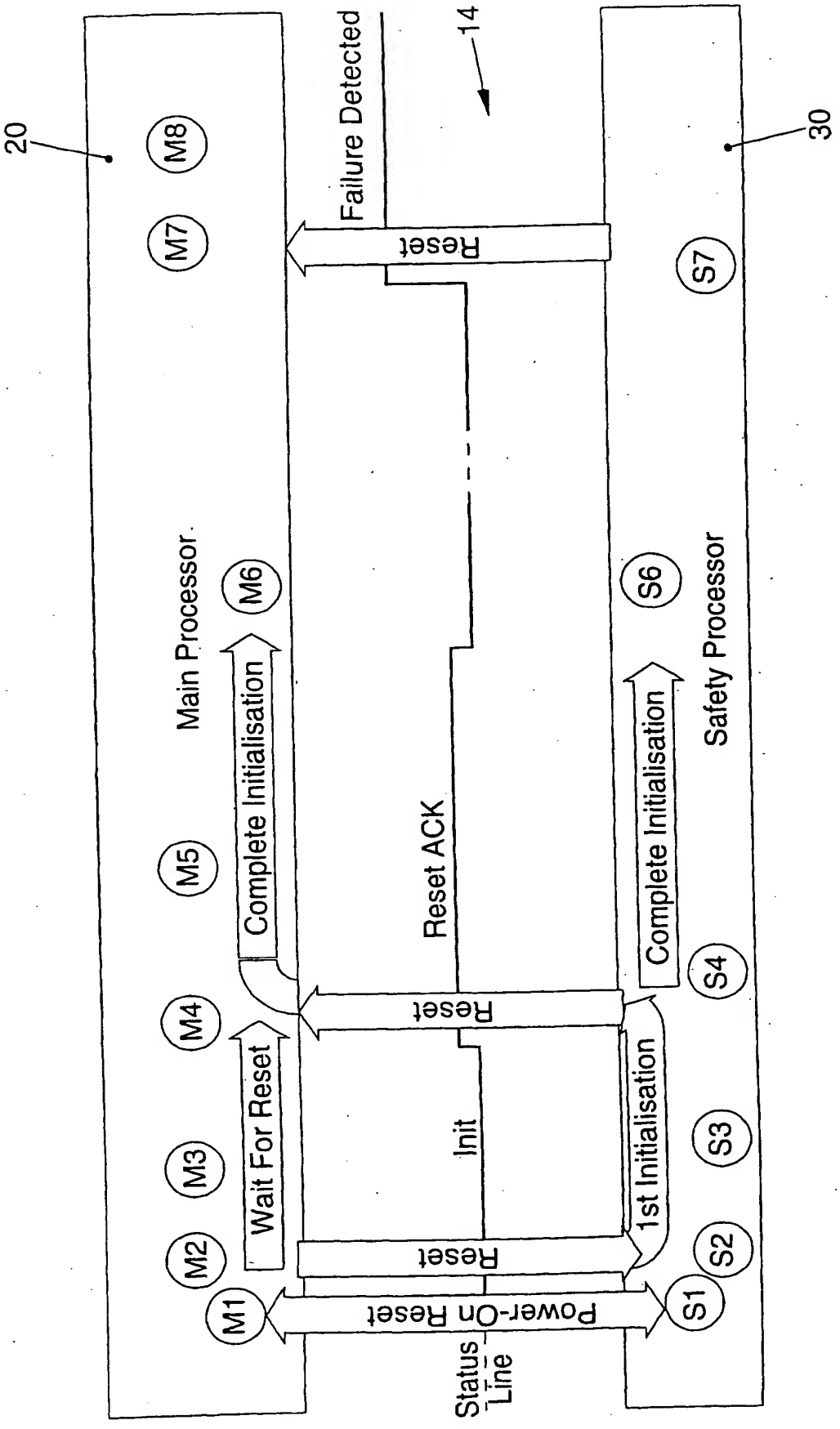
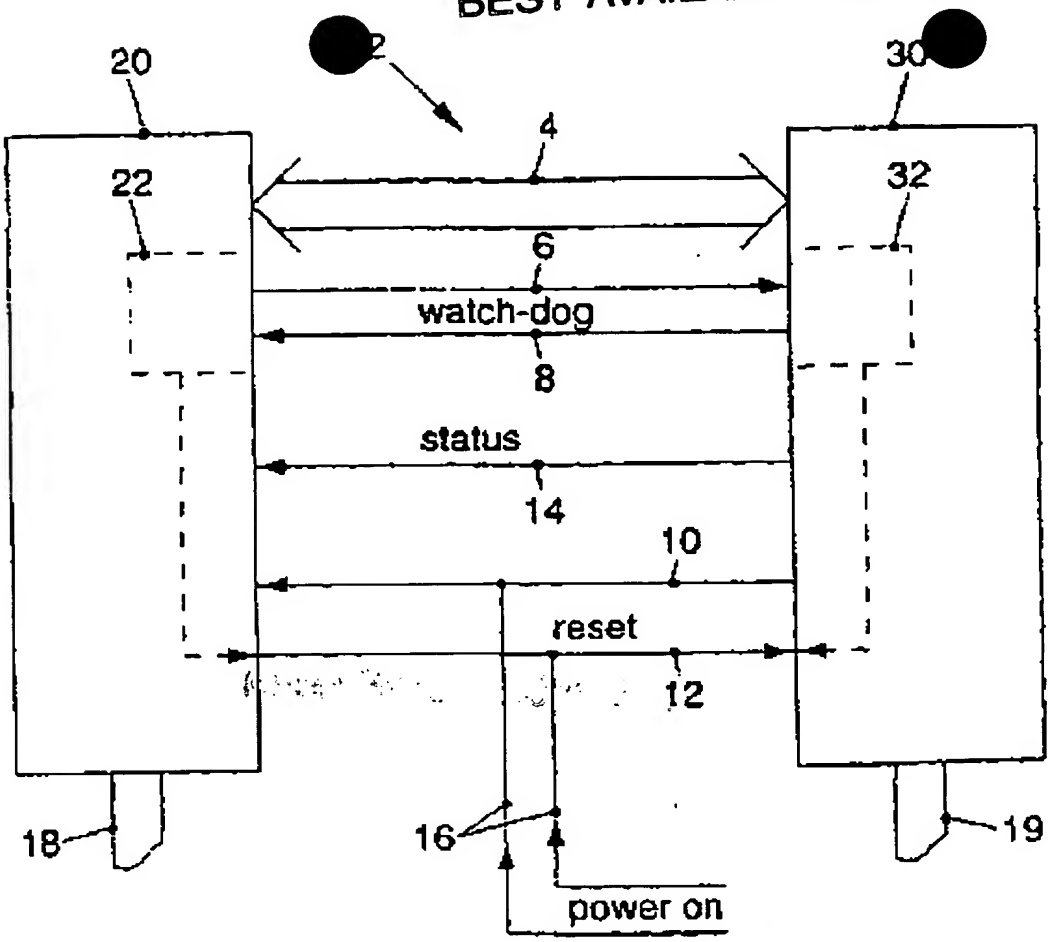


FIG. 2

AN: PAT 2003-45902[redacted]
TI: Computer error monitoring method e.g. for motor vehicle electronic control and braking systems, involves transmitting reset pulse via signal lines when error state of computer unit is detected
PN: **DE10151012**-A1
PD: 17.04.2003
AB: NOVELTY - A method of monitoring a computer system with first and second computing units (20,30) between which data and/or control signals are transmitted via first signal lines (6,8). When an error state of one of the computer units (20;30) is detected by the other computer unit (30;20) a reset pulse is transmitted from the other computer unit via second signal lines (12,10) to re-start afresh the one computer unit (20;30). During installation of the computer system (2), the latter is initialized by supplying a reset pulse (power-on-reset) to the computer units (20,30), and during the initialization process during installation of the computer system, the function of mutual starting of the computer units (20,30) afresh is checked for errors by transmitting reset pulses via the second signal lines (10,12). DETAILED DESCRIPTION - An INDEPENDENT CLAIM is given for a computer system with two computer units.; USE - For safety functions, such as electronic engine control and electronic braking systems in motor vehicles. ADVANTAGE - Greater functional safety of the computer system. DESCRIPTION OF DRAWING(S) - A much simplified block circuit diagram of a computer system is given. Computer system 2 Data- and control-bus 4 First signal lines 6,8 Second signal lines 10,12 Power-on reset signal line 16 Error detection devices 22,32
PA: (VOLS) VOLKSWAGEN AG;
IN: ALTENKIRCH M; KLINKIG A; LOEHNER A;
FA: **DE10151012**-A1 17.04.2003;
CO: DE;
IC: G06F-001/24; G06F-011/30;
MC: T01-G03; T01-J07D1; X22-C02D;
DC: T01; X22;
FN: 2003459027.gif
PR: DE1051012 16.10.2001;
FP: 17.04.2003
UP: 10.07.2003



THIS PAGE BLANK (USPTO)

DOCKET NO: S3-02P14830
SERIAL NO: 10/535,126
APPLICANT: Graßhoff et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100